

Primeros pasos de gestión de riesgo de ciberseguridad | *Ransomware*

Guía de inicio rápido

Con la creciente amenaza del *ransomware*, esta “guía de inicio rápido” ayudará a las organizaciones a utilizar la **Gestión de riesgo de ransomware: un perfil de marco de ciberseguridad** del Instituto Nacional de Normas y Tecnología (NIST) para combatir el *ransomware*. Al igual que el más amplio **Marco de ciberseguridad de NIST**, que es una guía voluntaria ampliamente utilizada para ayudar a las organizaciones a gestionar mejor y reducir el riesgo de ciberseguridad, el perfil de *ransomware* personalizado fomenta las comunicaciones y las acciones basadas en riesgos entre partes interesadas internas y externas, incluidos asociados y proveedores.

El marco está organizado en cinco funciones clave: identificar, proteger, detectar, responder y recuperar. Estos cinco términos proporcionan una visión integral del ciclo de vida para la gestión del riesgo de ciberseguridad. Las actividades enumeradas debajo de cada función ofrecen un buen punto de inicio para cualquier organización, incluyendo aquellas con recursos limitados para enfrentar desafíos de ciberseguridad. Ayudan a establecer prioridades para que una organización obtenga el máximo valor de sus esfuerzos para gestionar los riesgos de *ransomware*. Mucho depende de cuán sofisticadas sean sus operaciones actuales en términos de gestión de riesgos de ciberseguridad. Si bien hay muchas otras cosas que se pueden y se deben hacer para combatir el *ransomware*, es importante reconocer que no es necesario hacerlo todo de una vez. *Dar los primeros pasos es la clave en la ciberseguridad, ¡incluida la gestión de los riesgos de ransomware!* NIST recomienda seguir estos pasos para ayudar a impedir el *ransomware*...



IDENTIFICAR

Desarrollar una comprensión organizacional para la gestión del riesgo de ciberseguridad de: sistemas, activos, datos y capacidades.

- ➔ **Mantener inventarios de hardware y software.** Es importante comprender qué hardware y software informático utiliza su empresa. Estos son con frecuencia los puntos de entrada de actores maliciosos que participan en ataques de *ransomware*. Esta información apoya la remediación de vulnerabilidades que pueden aprovecharse en ataques de *ransomware* y también es muy útil en la recuperación. Este inventario puede ser tan simple como una hoja de cálculo. Los inventarios de software deberían hacer seguimiento de información como el nombre y la versión del software, los dispositivos en donde está instalado actualmente, la última fecha de actualización de parches y las vulnerabilidades conocidas.
- ➔ **Documentar los flujos de información.** Conocer qué tipo de información su empresa recolecta y utiliza es vital, pero también lo es comprender dónde están ubicados los datos y cómo fluyen, especialmente cuando hay contratos y compromisos con asociados externos. Cree un registro de flujos de información (p. ej., conexiones entre dispositivos/direcciones de protocolo de internet) para

ayudar a enumerar qué información o procesos están en riesgo si los atacantes se mueven lateralmente dentro de un entorno.

- ➔ **Identificar los sistemas de información externos a los que se conecta su empresa.** En caso de un evento de *ransomware*, debe planificar cómo se comunicará con los asociados e identificar posibles acciones para desconectarse temporalmente de los sistemas externos. Identificar estas conexiones también ayudará a la implementación de controles de seguridad (p. ej., derechos de acceso) y a indicar áreas donde los controles puedan compartirse con terceros.
- ➔ **Identificar los procesos y activos críticos de la empresa.** ¿Cuáles son las actividades empresariales que absolutamente deben continuar para que sea viable? Esto podría ser mantener un sitio web para obtener pagos, proteger información de clientes/pacientes de manera segura o garantizar que los datos que su empresa recolecta permanezcan accesibles y correctos. Esta información es esencial para comprender el verdadero alcance y efecto de los eventos de *ransomware* —y es importante en la planificación de contingencias para futuros eventos de *ransomware*, respuestas a emergencias y acciones de recuperación. Tener esta información de antemano permite a las empresas priorizar los recursos. Si cuenta con un sistema de control industrial (ICS), incluya sus funciones críticas.

- **Establecer políticas de ciberseguridad que detallen roles y responsabilidades.** Estas deben describir claramente sus expectativas sobre cómo las actividades de ciberseguridad, incluyendo las acciones de empleados, contratistas y asociados, protegerán su información y sistemas y apoyarán los procesos empresariales críticos. Las políticas de ciberseguridad deben integrarse con otras consideraciones de riesgo empresarial (p. ej., financieras, reputacionales).



- **Gestionar el acceso a los activos y la información.** Si no hace nada más, limite el acceso de los usuarios, procesos y dispositivos autorizados a los activos físicos y lógicos e instalaciones asociadas y gestione el acceso a actividades y transacciones críticas de acuerdo con el riesgo.

Comience creando cuentas únicas para cada empleado y garantice que los usuarios sólo tengan acceso a la información, los computadores y las aplicaciones que necesiten para sus labores. Utilice cuentas de usuario estándar con autenticación multifactorial en vez de cuentas con privilegios administrativos siempre que sea posible. Autentique a los usuarios mediante contraseñas seguras o técnicas multifactoriales antes de que les sea otorgado ese acceso.

Dado que la mayoría de los ataques de *ransomware* son realizados de manera remota, controlar el acceso remoto es vital para mantener la integridad de los sistemas y los archivos de datos para proteger de la inserción de código malicioso y la exfiltración de datos. Restrinja el acceso a redes oficiales desde dispositivos personales. Gestione y haga seguimiento estricto del acceso físico a los dispositivos, ya sea una computadora portátil o un componente crítico de un sistema de control industrial (ICS).

En organizaciones más grandes o complejas, la segregación o segmentación de redes puede limitar el alcance de los eventos de *ransomware* al evitar que el *malware* prolifere entre los potenciales sistemas objetivo. Esto es particularmente importante para las funciones críticas de un ICS, incluyendo los Sistemas Instrumentados de Seguridad (SIS).

- **Gestionar las vulnerabilidades de los dispositivos.** De manera regular, actualice los sistemas operativos y las

aplicaciones en sus computadores y otros dispositivos para protegerlos de ataques. ¡Manténgalos con todas las actualizaciones de parches instaladas! En lo posible, active las actualizaciones automáticas. Bloquee el acceso a sitios de *ransomware*. Considere el uso de herramientas de software para escanear dispositivos para buscar vulnerabilidades adicionales y remediar vulnerabilidades con altas probabilidades o efectos. La configuración debida de procesos de cambio y actualización puede ayudar a desalentar el reemplazo de código con productos que contienen *malware* o que no cumplen las políticas de gestión de acceso.

- **Educar y capacitar a los empleados y otros usuarios.** Capacite y vuelva a capacitar de manera habitual a todos los usuarios para que esté seguro de que están al tanto de las políticas y procedimientos empresariales de ciberseguridad y de sus roles y responsabilidades específicos y hágalo una condición de empleo. Capacitar a los responsables de la instalación, configuración y mantenimiento de hardware y software es clave, pero es igualmente importante capacitar a todos los usuarios para que usen siempre software antivirus, para instalar solo si están aprobados por la organización, hacer clic solo en enlaces verificados, para conectarse solo a redes seguras y no conectar dispositivos a estaciones de carga pública. Los usuarios deberían saber que su acceso a redes oficiales desde dispositivos personales está restringido. La mayoría de los ataques de *ransomware* son posibles debido a que hay usuarios que utilizan prácticas inseguras, administradores que implementan configuraciones inseguras o desarrolladores que no tienen la suficiente capacitación en seguridad.
- **Proteger sus dispositivos de forma segura.** Considere instalar cortafuegos con base en nodos de la red y otras protecciones como productos de seguridad de punto final. Aplique configuraciones uniformes a los dispositivos y controle los cambios a las configuraciones de dispositivos. Desactive los servicios o las características de dispositivos que no sean necesarios para apoyar las funciones de su misión. Garantice que haya una política y que los dispositivos sean eliminados de manera segura. Estas medidas protegen contra la instalación de *ransomware* y también protegen contra fugas de datos.
- **Proteger datos sensibles.** Es probable que su organización almacene o transmita datos sensibles, por lo que debe administrar su información y los registros (datos) según su estrategia de riesgo de la organización para proteger la confidencialidad, la integridad y la disponibilidad de la información. Use mecanismos de verificación de integridad (como firmas digitales) para verificar software, firmware e integridad de información y detectar actualizaciones de software alteradas que

puedan utilizarse para introducir un *malware*.

- ➔ **Realizar respaldos periódicos.** Garantizar la disponibilidad de datos puede reducir los efectos de *ransomware*. Esto incluye la capacidad de mantener respaldos de datos fuera del sitio y fuera de línea así como probar tiempos promedios de recuperación y redundancia de sistemas. Muchos sistemas operativos tienen capacidades integradas para hacer respaldos; también hay soluciones de software y en la nube disponibles para automatizar los respaldos. Es una buena práctica frecuentemente mantener un conjunto de datos respaldados fuera de línea. Los respaldos regulares que se mantienen y prueban son esenciales para la recuperación oportuna y relativamente sin complicaciones de los eventos de *ransomware*. Asegure las copias de seguridad y manténgalas fuera de línea para que no las corrompa ni las elimine un *ransomware* o un atacante.



DETECTAR

Desarrollar e implementar las actividades apropiadas para identificar cuando ocurra un evento de ciberseguridad.

- ➔ **Probar y actualizar procesos de detección.** Desarrolle y pruebe procesos y procedimientos para la detección de eventos anómalos como entidades y acciones no autorizadas en las redes y el entorno físico, incluyendo la actividad del personal. Esto incluye determinar el efecto de los eventos que pueden suministrar información para prioridades de respuesta y recuperación de un ataque de *ransomware*.

Las organizaciones más grandes o complejas deberían adquirir e instalar soluciones de seguridad de información y gestión de eventos (SIEM) que incluyan fuentes y sensores para mejorar la visibilidad de la red, apoyar la detección temprana de *ransomware* y ayudar en la comprensión de cómo el *ransomware* puede propagarse a través de una red. Estas herramientas necesitan generar y registrar (archivo de registro o logs) la actividad. Los archivos de registro son cruciales para identificar anomalías en computadores y aplicaciones; registran eventos como cambios a sistemas o cuentas así como canales de comunicación. Considere el uso de herramientas de software que puedan acumular estos archivos de registro y buscar patrones o anomalías del comportamiento de red esperado.

- ➔ **Capacitar el personal.** El personal debe estar al tanto de sus roles y responsabilidades para detectar y reportar dentro de su organización y hacia las autoridades externas. Eso requiere capacitar y volver a capacitar.

- ➔ **Conocer los flujos de datos esperados.** Si usted sabe qué datos y cómo se espera que fluyan en su empresa, tendrá mayor probabilidad de notar cuando algo inesperado ocurra y lo inesperado nunca es bueno cuando se trata de la ciberseguridad. Los flujos de datos inesperados pueden incluir información de clientes que se exporta desde una base de datos interna y que sale de la red. Si ha contratado trabajo en la nube o a un proveedor de servicio administrado, converse con ellos sobre cómo hacen seguimiento de los flujos de datos y reportes, incluyendo eventos inesperados.

- ➔ **Comunicar rápidamente y determinar el efecto de los eventos de ciberseguridad.** La comunicación oportuna de eventos anómalos es necesaria para poder llevar a cabo acciones de remediación antes de que un ataque de *ransomware* pueda ser completamente dañino. Si se detecta un evento de ciberseguridad, su empresa debe trabajar rápida y exhaustivamente para comprender la amplitud y profundidad del efecto. Busque ayuda. Comunicarse con las partes interesadas apropiadas y con las fuerzas del orden (por ejemplo, el FBI) puede ayudarlo a mantenerse en buenos términos con sus asociados, entidades supervisoras y otros (potencialmente incluyendo inversionistas) y mejorar políticas y procedimientos.



RESPONDER

Desarrollar e implementar las actividades apropiadas para tomar acción en relación con un evento de ciberseguridad detectado.

- ➔ **Desarrollar planes de respuesta.** Como muchas otras cosas, la respuesta a *ransomware* comienza con la planificación, incluida la coordinación de planes con partes interesadas internas y externas. Concéntrese en los procedimientos para la mitigación inmediata y la contención del evento de *ransomware* y la determinación de su efecto.
- ➔ **Coordinar con las partes interesadas internas y externas.** Incluya a todos los proveedores de servicio externos y todas las partes interesadas clave. Mantenga una lista actualizada de contactos internos y externos para el caso de ataques de *ransomware*, incluyendo

recursos de las fuerzas del orden, asesoría legal y respuesta a incidentes. Las prioridades incluyen mensajes preventivos y acuerdos sobre cómo detener la difusión de información errónea. Las partes interesadas pueden contribuir a mejoras en la planeación y la ejecución.

- ➔ **Probar planes de respuesta.** Las pruebas ayudan a asegurarse de que cada persona sepa sus responsabilidades en la ejecución del plan. Cuanto mejor preparada esté su organización, más eficaz será la respuesta. Esto incluye conocer cualesquiera requerimientos legales de presentación de informes o intercambio de información requerido.
- ➔ **Actualizar los planes de respuesta.** Probar el plan (y la ejecución durante un incidente) inevitablemente revelarán mejoras necesarias. Asegúrese de actualizar los planes de respuesta con las lecciones aprendidas. Esto minimizará la probabilidad de futuros ataques de *ransomware* exitosos y ayudará a restablecer la confianza entre las partes interesadas.



RECUPERAR

Desarrollar e implementar las actividades apropiadas para mantener planes para la resiliencia y para reestablecer cualesquiera capacidades o servicios que hayan sido afectados durante un evento de ciberseguridad.

- ➔ **Hacer planes de contingencia.** Al igual que la respuesta, la recuperación de eventos de *ransomware* comienza con la planificación de contingencia mucho antes de un evento. En este caso, su empresa debe planificar la restauración de las capacidades de los sistemas y la corrección de vulnerabilidades. Concéntrese en los procedimientos para la mitigación inmediata del evento de *ransomware*, la determinación del efecto del evento y la notificación con las partes interesadas.
- ➔ **Comunicarse con las partes interesadas internas y externas.** La recuperación depende de la comunicación efectiva. Sus planes de recuperación necesitan dar cuenta cuidadosamente de qué, cómo y cuándo se compartirá la información de eventos de *ransomware* con diversas partes interesadas para que todas las partes interesadas reciban la información que necesitan, pero que no se comparta ninguna información inapropiada.
- ➔ **Gestionar las relaciones públicas y la reputación de la compañía.** Cuando desarrolle un plan de recuperación de *ransomware*, considere cómo hará la gestión de relaciones públicas para que el intercambio de información sea preciso, completo y oportuno —y no reaccionario.
- ➔ **Probar y actualizar los planes de recuperación.** Probar la ejecución de los planes de recuperación mejorará la conciencia de los empleados y asociados en cuanto a estos planes y resaltarán las áreas de mejora. Siempre actualice los planes con las lecciones aprendidas.

DÓNDE ENCONTRAR MÁS RECURSOS DE RANSOMWARE DE NIST...

- ✓ **RECURSOS DE PROTECCIÓN Y RESPUESTA:**
<https://csrc.nist.gov/projects/ransomware-protection-and-response>
- ✓ **EL RINCÓN DE CIBERSEGURIDAD DE NIST PARA PEQUEÑAS EMPRESAS:**
<https://www.nist.gov/itl/smallbusinesscyber/guidance-topic/ransomware>
- ✓ **HOJA DE CONSEJOS Y TÁCTICAS:**
<https://www.nist.gov/itl/smallbusinesscyber/guidance-topic/ransomware>

¿PREGUNTAS? Escribanos un correo electrónico a: ransomware@nist.gov

Document translated courtesy of U.S. Department of State with support from the **Digital Connectivity and Cybersecurity Partnership (DCCP)**. Official U.S. Government Translation.

The official English language version of this publication is available free of charge from the National Institute of Standards and Technology (NIST): <https://www.nist.gov/publications>.

Última actualización: febrero de 2022